DISCIPLINE: Identification and Authentication

Discipline Roadmap for: Enterprise Single Sign-On (ESSO)

DOMAIN: SECURITY

Current	2 Years	5 Years
Baseline Environment	**Tactical Deployment**	**Strategic Direction**
Novell →		Market watch of ESSO and IAM (identity and access management) best practices and solutions.
Imprivata →		
CA →		
Citrix →		
Actividentity →		
Open Source SSO (e.g. Sun, JOSSO, Shibboleth) →		
Passlogix →		

Shared	Agency
	✓

Retirement Targets

N/A

Mainstream Platforms (must be supported)

Novell, Imprivata, CA, Citrix, Actividentity, Open Source SSO, Passlogix

Containment Targets

N/A

Emerging Platforms

Market Watch

Implications and Dependencies

- User access and authorization through RDMS or LDAP based systems.
- Management through SNMPv3 or IP.

Roadmap Notes

- Standard to reviewed annually after adoption by the AOC.

DISCIPLINE: Identification and Authentication

Discipline Roadmap for: Enterprise Single Sign-On (ESSO)

- **Discipline Boundaries:**
  - Enterprise Single Sign-On refers to specialized software that enables a user to authenticate once and gain access to multiple, often disparate, technology targets (e.g. network, web, and windows interfaces). ESSO is part of a larger segment of tools known as identity and access management (IAM), but it is differentiated from similar technologies (such as password wallets, password synchronization, and directory sign-on) because it is centrally administered on an enterprise level, provides automatic log on, and allows for legacy applications that are not directory-enabled.
- **Discipline Standards:**
  - Currently, there are no generally accepted independent standards. Instead, ESSO tools are proprietary, although some use XML as an integral part of their system. However, the Federal Government has adopted the Organization for the Advancement of Structured Information Standards (OASIS) Security Assertion Markup Language (SAML) as its base standard.
- **Migration Considerations:**
  - Migration can be expensive and time consuming.
  - Positive ROI, through user and helpdesk time savings, is generally not realized unless an entity has several heterogeneous applications requiring daily sign-on with individualized credentials.
  - Can be coupled with other authentication methods, such as biometrics or smart cards, to provide stronger authentication in order to address concerns that a compromise of the master password likewise compromises all target systems.
  - Consider “webifying” legacy applications in order to exploit WAM (web access management) products as newer applications are usually natively web-enabled.
- **Exception Considerations:**
  - Specialized business needs requiring exception should to be reviewed through the AOC exception process.
- **Miscellaneous Notes:**
  - None
- **Established**
  - November 15, 2006
- **Date Last Updated:**
  - November 15, 2006
- **Next Review Date:**
  - November 2007